Constructive Provability Logic

Robert J. Simmons
and
Bernardo Toninho

We present *constructive provability logic*, an intuitionstic modal logic that validates the Löb rule of Gödel and Löb's provability logic by permitting logical reflection over provability. Two distinct variants of this logic, **CPL** and **CPL***, are presented in natural deduction and sequent calculus forms which are then shown to be equivalent. In addition, we discuss the use of constructive provability logic to justify stratified negation in logic programming within an intuitionstic and structural proof theory.

All theorems presented in this paper are formalized in the Agda proof assistant. An earlier version of this work was presented at IMLA 2011 [Simmons and Toninho 2011].

Draft as of March 5, 2013

Consider the following propositions (where "⊃" represents implication):

$$\forall x.\, \forall y.\, \mathsf{edge}(x, y) \supset \mathsf{edge}(y, x)$$
$$\forall x.\, \forall y.\, \mathsf{edge}(x, y) \supset \mathsf{path}(x, y)$$
$$\forall x.\, \forall y.\, \forall z.\, \mathsf{edge}(x, y) \supset \mathsf{path}(y, z) \supset \mathsf{path}(x, z)$$

One way to think of these propositions is as rules in a *bottom-up logic program*. This gives them an operational meaning: given some known set of facts, a bottom-up logic program uses rules to derive more facts. If we start with the single fact $\mathsf{edge}(\mathsf{a}, \mathsf{b})$, we can derive $\mathsf{edge}(\mathsf{b}, \mathsf{a})$ by using the first rule (taking $x = \mathsf{a}$ and $y = \mathsf{b}$), and then, using this new fact, we can derive $\mathsf{path}(\mathsf{b}, \mathsf{a})$ by using the second rule (taking $x = \mathsf{b}$ and $y = \mathsf{a}$). Finally, from the original $\mathsf{edge}(\mathsf{a}, \mathsf{b})$ fact and the new $\mathsf{path}(\mathsf{b}, \mathsf{a})$ fact, we can derive $\mathsf{path}(\mathsf{a}, \mathsf{a})$ using the third rule (taking $x = \mathsf{a}$, $y = \mathsf{b}$, and $z = \mathsf{a}$). Once the only new facts we can derive are facts we already know, we say we have reached *saturation* — this will happen in our example when we have derived $\mathsf{edge}(\mathsf{a}, \mathsf{b})$, $\mathsf{edge}(\mathsf{b}, \mathsf{a})$, $\mathsf{path}(\mathsf{a}, \mathsf{b})$, $\mathsf{path}(\mathsf{b}, \mathsf{a})$, $\mathsf{path}(\mathsf{a}, \mathsf{a})$, and $\mathsf{path}(\mathsf{b}, \mathsf{b})$. Bottom-up logic programming is a very simple and intuitive kind of reasoning, and it has also shown to be an elegant and powerful way of declaratively specifying and efficiently solving many computational problems, especially in the field of program analysis (see [Whaley et al. 2005] for a number of references).

Next, consider the following proposition:

$$\forall x.\, \forall y.\, \mathsf{path}(x, y) \supset \neg\mathsf{edge}(x, y) \supset \mathsf{noedge}(x, y)$$

Intuition says that this is a meaningful statement. In our example above, we can derive $\mathsf{path}(\mathsf{a}, \mathsf{a})$, but we can't possibly derive $\mathsf{edge}(\mathsf{a}, \mathsf{a})$, so we should be able to conclude $\mathsf{noedge}(\mathsf{a}, \mathsf{a})$. A bottom-up logic programming semantics based on *stratified negation* verifies this intuition [Przymusinski 1988]. In a stratified logic program made up of the four previous rules, we can derive all the consequences of the first three rules until saturation is reached. At this point, we know everything there is to know about facts of the form $\mathsf{edge}(X, Y)$ and $\mathsf{path}(X, Y)$. When considering the negated premise $\neg\mathsf{edge}(x, y)$ in the fourth rule, we simply check the saturated database and conclude that the premise holds if the fact does not appear in the database.

Stratified negation would, however, disallow the addition of the following rule as paradoxical or contradictory:

$$\forall x. \forall y. \mathsf{path}(x, y) \supset \neg\mathsf{edge}(x, y) \supset \mathsf{edge}(x, y)$$

Why is this rule problematic? Operationally, the procedure we used for stratified negation no longer really makes sense: we reach saturation, then conclude that there was no way to prove $\mathsf{edge}(\mathsf{a}, \mathsf{a})$, then use that conclusion to prove $\mathsf{edge}(\mathsf{a}, \mathsf{a})$. But we had just concluded that it wasn't provable! Stratified negation ensures that we never use the fact that there is no proof of A to come up with a proof of A, either directly or indirectly. However, stratified negation is an odd property: the program consisting of the single rule $\neg\mathsf{prop1} \supset \mathsf{prop2}$ is stratified (we consider $\mathsf{prop1}$ first, and then we consider $\mathsf{prop2}$), and the program consisting of the single rule $\neg\mathsf{prop2} \supset \mathsf{prop1}$ is also stratified (we consider $\mathsf{prop2}$ first, and then we consider $\mathsf{prop1}$), but the two rules cannot be combined as a single stratified logic program.

In part due to this non-compositional nature, stratified negation in logic programming has thus far eluded a treatment by the tools of structural proof theory. Instead, justifications of negation in logic programming have universally been of a classical nature based on the assignment of truth values (Boolean, three-valued, or otherwise) to atomic propositions. In this paper, we take a first step towards a structurally proof-theoretic justification of stratified negation in which computation is understood as proof search for *uniform* (or *focused*) proofs [Miller et al. 1991; Andreoli 1992]. The logic that we present has strong ties to **GL**, the Gödel-Löb logic of provability [Verbrugge 2010],[1] and we therefore call it *constructive provability logic*. This connection in our intuitionistic setting was anticipated by Gabbay [1991], who showed that **GL** was a natural choice for justifying negation in a classical, model-theoretic account of logic programming.

Outline

Logic programming is our primary motivation, but this article will mostly focus on constructive provability logic *as a logic*. In Section 1, we develop the ideas behind constructive provability logic. There are two natural variants of constructive provability logic with different properties. The "tethered" variant of constructive provability logic, **CPL**, is discussed in Section 2. The "de-tethered" variant of constructive provability logic, **CPL***, is discussed in Section 3, and in Section 4 we sketch the use of **CPL*** as a logic programming language. In Section 5 we consider the relationship between this logic and classical Hilbert-style presentations of provability logic, and we conclude in Section 6.

In the course of this paper we will give both natural deduction and sequent calculus presentations of **CPL** and **CPL***, and show that, for each logic, the natural deduction and sequent calculus presentations are equivalent at the level of provability. Natural deduction presentations are the most typical way of thinking about proofs and their reductions. Sequent calculus presentations, on the other hand, are

[1] **GL** is also known variously in the literature as **G**, **L**, **Pr**, **PrL**, **KW**, and **K4W**.

more useful for proving negative statements about the logic (i.e. that a certain fact is *not* provable); such statements come up frequently in the way we use constructive provability logic.

1. A JUDGMENTAL RECONSTRUCTION OF PROVABILITY LOGIC

In this section we provide a very brief introduction to the judgmental methodology that informs our development of constructive provability logic. Our presentation is consistent with Pfenning and Davies' judgmental reconstruction of modal logic [Pfenning and Davies 2001], which in turn follows Martin Löf's 1983 Siena Lectures [Martin-Löf 1996].

The key concept behind the judgmental methodology is the separation between propositions (written A, B, etc.) and judgments J. A proposition is a syntactic object that is built up from *atomic propositions* using propositional connectives such as implication and conjunction. Judgments are proved through rules of inference. Thus, we can talk about proving the judgment A *true* or the judgment A *false*. It is not meaningful to talk about "proving A" except as a shorthand way of talking about proving the judgment A *true*.

When proving a particular judgment, one should be able to reason from hypotheses. To this end, the concept of an *hypothetical* judgment, written $J_1, \ldots, J_n \vdash J$, comes into play. The conventional interpretation of such a hypothetical judgment is that J has a proof under the assumptions that J_1 through J_n also have proofs. However, the meaning of a hypothetical judgment is not given to us *a priori*. Rather, we *define* the meaning of a hypothetical judgment by defining (1) a *hypothesis* principle, (2) a *generalized weakening* principle, and a (3) *substitution* principle. These principles arise from the understanding of what a given hypothetical judgment should mean. The hypothesis principle defines how hypothetical assumptions are used. The generalized weakening principle defines primitive operations on hypothetical assumptions that do not change the meaning of a judgment (e.g. "the order in which we write assumptions does not matter", "all assumptions need not be used in a proof"). Finally, the substitution principle defines the conditions under which reasoning through lemmas is justified.

Plain-vanilla intuitionistic logic is one of the so-called *structural logics*, and as a structural logic its defining principles are simple and standard:

Defining principles of plain-vanilla intuitionistic logic:

—*Hypothesis principle*: If $A\ \mathit{true} \in \Psi$, then $\Psi \vdash A\ \mathit{true}$.

—*Generalized weakening principle*: If $\Psi \subseteq \Psi'$ and $\Psi \vdash A\ \mathit{true}$, then $\Psi' \vdash A\ \mathit{true}$.

—*Substitution principle*: If $\Psi \vdash A\ \mathit{true}$ and $\Psi, A\ \mathit{true} \vdash C\ \mathit{true}$, then $\Psi \vdash C\ \mathit{true}$.

These principles have an interesting character. While they are, in some sense, the last thing we need to consider when defining a logic (i.e. after defining the logic, they are theorems we need to prove about the system), the judgmental methodology tells us that these principles are also the *first* things that need to be considered. Philosophically, this arises from the fact that these principles flow from our understanding of the meaning of the hypothetical judgment. More pragmatically, generalized weakening and substitution are necessary as we perform sanity checks on the rules that define individual connectives.

1.1 Natural deduction in the judgmental methodology

The judgmental methodology is generally played out in the setting of natural deduction. In natural deduction, the meaning of a logical connective is given by two sets of rules: the *introduction* rules, stating how we can come to know (that is, prove) of the truth of that connective, and the *elimination* rules, defining how we can use the knowledge (that is, the proof) of that proposition's truth. For instance, implication $A \supset B$ is defined by one introduction rule $\supset I$ and one elimination rule $\supset E$:

$$\frac{\Psi, A\ \mathit{true} \vdash B\ \mathit{true}}{\Psi \vdash A \supset B\ \mathit{true}} \supset I \qquad \frac{\Psi \vdash A \supset B\ \mathit{true} \quad \Psi \vdash A\ \mathit{true}}{\Psi \vdash B\ \mathit{true}} \supset E$$

In natural deduction, the sanity checks that we perform on a definition like this are called *local soundness* and *local completeness*. Local soundness ensures that the introduction rules are strong enough with respect to the elimination rules, whereas local completeness ensures that the introduction rules are not too strong with respect to the elimination rules.

Local soundness. Consider a proof $\mathcal{D}$ of the judgment $\Psi \vdash C\ \mathit{true}$ where the last rule is an elimination rule (in the case for implication, the elimination rule is $\supset E$ and so we have two subproofs, one of $\Psi \vdash A \supset C\ \mathit{true}$ – call it $\mathcal{D}_1$ – and another of $\Psi \vdash A\ \mathit{true}$ – call it $\mathcal{D}_2$). Since the rule is an elimination rule, it is necessarily the case that one of the subproofs mentions the relevant connective (in the case for implication, the first sub-proof $\mathcal{D}_1$ mentions the connective). Local soundness is the property that, if the last rule in the connective-mentioning premise is an introduction rule, then both the introduction rule and the elimination are unnecessary. To show this, we build a proof of $\Psi \vdash C\ \mathit{true}$ using only the premises of the introduction rule and any other premises of the elimination rule. In our example with implication, we can obtain this new proof by appealing to the substitution principle for the subproofs labeled $\mathcal{D}_2$ and $\mathcal{D}_1'$:

$$\dfrac{\dfrac{\begin{matrix}\mathcal{D}_1' \\ \Psi, u : A\ \mathit{true} \vdash C\ \mathit{true}\end{matrix}}{\Psi \vdash A \supset C\ \mathit{true}} \supset I \qquad \begin{matrix}\mathcal{D}_2 \\ \Psi \vdash A\ \mathit{true}\end{matrix}}{\Psi \vdash C\ \mathit{true}} \supset E \qquad \Longrightarrow_R \qquad \begin{matrix}[\mathcal{D}_2/u]\mathcal{D}_1' \\ \Psi \vdash C\ \mathit{true}\end{matrix}$$

Note that, following standard conventions, we gave the label u to the premise $A\ \mathit{true}$ in the hypothetical judgment to make it clear what we were substituting for.

Local completeness. Where local soundness is witnessed by a proof reduction, local completeness is witnessed by a proof expansion: given an arbitrary proof of the truth of connective we are interested in, we show that by applying the elimination rules and then applying the introduction rules we can reconstruct the initial proof. In the expansion below, we obtain $\mathcal{D}'$ by applying the generalized weakening principle to the given proof $\mathcal{D}$:

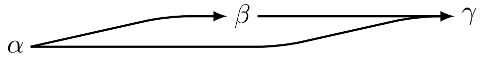
$$\begin{matrix}\mathcal{D} \\ \Psi \vdash A \supset B\ \mathit{true}\end{matrix} \qquad \Longrightarrow_E \qquad \dfrac{\dfrac{\begin{matrix}\mathcal{D}' \\ \Psi, A\ \mathit{true} \vdash A \supset B\ \mathit{true}\end{matrix} \qquad \dfrac{}{\Psi, A\ \mathit{true} \vdash A\ \mathit{true}}\ \mathit{hyp}}{\Psi, A\ \mathit{true} \vdash B\ \mathit{true}} \supset E}{\Psi \vdash A \supset B\ \mathit{true}} \supset I$$

We also used the hypothesis principle in the above example: in natural deduction systems, the hypothesis principle always holds trivially due the presence of the rule we labeled *hyp*.

1.2 Reflection over an accessibility relation

Having reviewed the judgmental methodology, we will now perform a sort of warm-up exercise to introduce the idea of definitional reflection in the presentation of a logic [Schroeder-Heister 1993]. This warm-up logic, which we name **DML** (for "**D**efinitional **M**odal **L**ogic"), is recognizably similar to **IK**, the intuitionistic Kripke semantics for modal logic presented by Simpson [1994].

Kripke semantics for modal logic are characterized by *worlds* and an *accessibility relation* that describes the relationship between worlds. We will use as a running example an accessibility relation with three worlds, α, β, and γ, such that $\alpha \prec \beta$ (we say "β is accessible from α"), $\alpha \prec \gamma$, and $\beta \prec \gamma$.



The proof theory of **DML** is parametrized over an arbitrary accessibility relation; the three-world accessibility relation above is only one possible example. The hypothetical judgment for this logic takes the form $A_1[w_1], \ldots, A_n[w_n] \vdash C[w]$, where C and the A_i are propositions and w and the w_i are worlds. **DML** is also a structural logic, so its judgmental principles are straightforward:

Defining principles of **DML***:*

—*Hypothesis principle*: If $A[w] \in \Gamma$, then $\Gamma \vdash A[w]$.

—*Generalized weakening principle*: If $\Gamma \subseteq \Gamma'$ and $\Gamma \vdash A[w]$, then $\Gamma' \vdash A[w]$.

—*Substitution principle*: If $\Gamma \vdash A[w]$ and $\Gamma, A[w] \vdash C[w']$, then $\Gamma \vdash C[w']$.

In **DML**, as in Simpson's **IK**, worlds and the accessibility relation are critical to the definition of the modal operators. Consider the definition of modal possibility, $\Diamond A$. The Kripke interpretation of modal possibility is that $\Diamond A$ is true at world w if there exists some accessible world w' where A is true. The introduction rule for modal possibility directly reflects this interpretation:

$$\frac{w \prec w' \quad \Gamma \vdash A[w']}{\Gamma \vdash \Diamond A[w]} \; \Diamond I$$

The elimination rule for modal possibility is where the use of definitional reflection becomes important. If we can prove that $\Diamond A$ is true at the world w, we can use case analysis over the pre-defined accessibility relation to look up all the worlds w' such that $w \prec w'$ holds; for each such w', we must prove the ultimate conclusion using the additional hypothesis $A[w']$. This is expressed by the following inference rule:

$$\frac{\Gamma \vdash \Diamond A[w] \quad \forall w'.\, w \prec w' \longrightarrow \Gamma, A[w'] \vdash C[w'']}{\Gamma \vdash C[w'']} \; \Diamond E$$

In our aforementioned example, there are two worlds w' such that $\alpha \prec w'$ holds. Therefore, to eliminate a proof of $\Diamond A[\alpha]$, we must consider the case where A holds at world β and the case where A holds at world γ. Similarly, because there are zero worlds w' such that $\gamma \prec w'$ holds, a proof of $\Diamond A[\gamma]$ is contradictory and can be used to prove anything at all. These two derivable special cases of the possibility elimination rule can be written as follows:

$$\frac{\Gamma \vdash \Diamond A[\alpha] \quad \Gamma, A[\beta] \vdash C[w''] \quad \Gamma, A[\gamma] \vdash C[w'']}{\Gamma \vdash C[w'']}\,\Diamond E_\alpha \qquad \frac{\Gamma \vdash \Diamond A[\gamma]}{\Gamma \vdash C[w'']}\,\Diamond E_\gamma$$

This elimination rule is what makes **DML** strikingly different, and seemingly stronger, than Simpson's **IK**. In **IK**, it would not be possible to prove $\cdot \vdash \Diamond A \supset \bot[\gamma]$, but in **DML** this is a simple use of the $\supset I$ and $\Diamond E_\gamma$ rules. This strength comes at a price, of course. Any reasoning in **IK** is valid in a larger accessibility relation, but in **DML**, the aforementioned hypothetical judgment $\cdot \vdash \Diamond A \supset \bot[\gamma]$ would no longer be valid if the accessibility relation was made larger in certain ways (for example, by making γ accessible from itself).

It is possible, at least in this simple case, to see $\Diamond E$ as merely a rule schema that, once given an accessibility relation, stamps out an appropriate number of rules. However, as suggested by Zeilberger [2008], it is more auspicious to take this higher-order formulation of definitional reflection at face value: the second premise of the $\Diamond E$ rule is actually a (meta-level) mapping – a function – from facts about the accessibility relation to derivations. This interpretation becomes relevant when we discuss local soundness.

To show local soundness, we use functional application to discharge the higher-order premises, so that $(\mathcal{D}_2\, w'\, \mathcal{A}_1)$ below is a derivation of the hypothetical judgment $\Gamma, u : A[w'] \vdash C[w'']$.

$$\cfrac{\cfrac{\overset{\mathcal{A}_1}{w \prec w'} \quad \overset{\mathcal{D}'_1}{\Gamma \vdash A[w']}}{\Gamma \vdash \Diamond A[w']}\,\Diamond I \qquad \overset{\mathcal{D}_2}{\forall w^*. w \prec w^* \longrightarrow \Gamma, u : A[w^*] \vdash C[w'']}}{\Gamma \vdash C[w'']}\,\Diamond E$$

$$\Longrightarrow_R \quad \begin{array}{c}[\mathcal{D}'_1/u](\mathcal{D}_2\, w'\, \mathcal{A}_1)\\ \Gamma \vdash C[w'']\end{array}$$

Local completeness is a bit difficult to write clearly in the traditional two-dimensional notation used for proofs. It begins like this:

$$\begin{array}{c}\mathcal{D}\\ \Gamma \vdash \Diamond A[w]\end{array} \quad \Longrightarrow_E \quad \frac{\overset{\mathcal{D}}{\Gamma \vdash \Diamond A[w]} \quad \overset{???}{\forall w'. w \prec w' \longrightarrow \Gamma, A[w'] \vdash \Diamond A[w]}}{\Gamma \vdash \Diamond A[w]}\,\Diamond E$$

We discharge the remaining proof obligation marked ??? above with a lemma: we must prove that for all w', $w \prec w'$ implies $\Gamma, A[w'] \vdash \Diamond A[w]$. If we label the given premise $w \prec w'$ as $\mathcal{A}$, this fact is be established by the following schematic derivation:

$$\cfrac{\overset{\mathcal{A}}{w \prec w'} \quad \cfrac{}{\Gamma, A[w'] \vdash A[w']}\,\mathit{hyp}}{\Gamma, A[w'] \vdash \Diamond A[w]}\,\Diamond I$$

This proves our lemma, which in turn suffices to show local completeness for modal possibility, ending our discussion of the system **DML**.

1.3 Reflection over provability

The system **DML** was just a warm-up that introduced reflection over the definition of an accessibility relation. We will now introduce constructive provability logic by additionally using reflection over provability. In **DML**, a proof of $\Diamond A[w]$ allows us to assume (by the addition of a new hypothetical assumption) that A is true at one of the worlds w' accessible from w; if there is no such world w', the assumption is contradictory. In constructive provability logic, a proof of $\Diamond A[w]$ will allow us to assume that A is *provable given the current set of hypotheses* at one of the worlds w' accessible from w. If A is not currently provable at some world w' accessible from w, the assumption is contradictory.

As a specific example, if Q is an arbitrary atomic proposition, $\bot$ is the proposition representing falsehood, and we use the accessibility relation from the previous section, then in constructive provability logic we can prove $\Diamond Q[\alpha] \vdash \bot[\alpha]$ by the use of reflection over logical provability. It is possible to show, using techniques that we will introduce later, that there is *no* proof of $\Diamond Q[\alpha] \vdash Q[\beta]$ and *no* proof of $\Diamond Q[\alpha] \vdash Q[\gamma]$. This, in turn, allows us to conclude that asserting that Q is currently provable at one of the worlds w' accessible from α is contradictory. The same judgment $\Diamond Q[\alpha] \vdash \bot[\alpha]$ would *not* have been provable in **DML**. In order to use a proof of $\Diamond Q[\alpha]$ in **DML**, we would have to prove both $\Diamond Q[\alpha], Q[\beta] \vdash \bot[\alpha]$ and $\Diamond Q[\alpha], Q[\gamma] \vdash \bot[\alpha]$, and neither of these hypothetical judgments are, in fact, provable.

1.3.1 *The weakening principle for constructive provability logic.* The discussion above is enough to make it clear that the generalized weakening principle from **DML** will not be acceptable for constructive provability logic. In **DML**, the weakening principle asserts that, if we can prove $\Gamma \vdash \bot[\alpha]$, then we can always also prove $\Gamma, Q[\beta] \vdash \bot[\alpha]$. Compare this to the previous discussion where we counted on there being no proof of the hypothetical judgment $\Diamond Q[\alpha] \vdash Q[\beta]$. If we weaken the context with the additional judgment $Q[\beta]$, we get a hypothetical judgment $\Diamond Q[\alpha], Q[\beta] \vdash Q[\beta]$ that *is* provable, invalidating our reasoning.

This illustrates that constructive provability logic must avoid some forms of weakening. To this end, we define a new partial order on contexts that is indexed by a world w, written as $\Gamma \subseteq_w \Gamma'$. This relation holds exactly when:

—For all w' such that $w \prec^* w'$, $A[w'] \in \Gamma$ implies $A[w'] \in \Gamma'$, and

—For all w' such that $w \prec^+ w'$, $A[w'] \in \Gamma'$ implies $A[w'] \in \Gamma$.

Here, $w \prec^* w'$ is the reflexive and transitive closure of the accessibility relation and $w \prec^+ w'$ is the transitive closure of the accessibility relation. This indexed subset relation $\subseteq_w$ acts like the normal subset relation when dealing with judgments $A[w]$, but for assumptions at worlds $A[w']$ where w' is transitively accessible from w, only contraction and exchange are allowed. Assumptions $A[w']$ where w' is neither equal to w nor transitively accessible from w are completely unconstrained and can be added or removed without restriction.

With our new partial order, we can present two of the defining principles of constructive provability logic.

Partial defining principles of constructive provability logic:

—*Hypothesis principle*: If $A[w] \in \Gamma$, then $\Gamma \vdash A[w]$.

—*Generalized weakening principle*: If $\Gamma \subseteq_w \Gamma'$ and $\Gamma \vdash A[w]$, then $\Gamma' \vdash A[w]$.

We omit the substitution principle for now, because it is different in the two different variants of constructive provability logic that we present in this paper.

1.3.2 *Restrictions on accessibility relations and the form of rules.* Reflection over provability must be done with care. It would be logically inconsistent to modify our previous elimination rule for modal possibility by turning the hypothesis $A[w']$ into a higher-order assumption $\Gamma \vdash A[w']$ like this:

$$\frac{\Gamma \vdash \Diamond A[w] \quad \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w'] \longrightarrow \Gamma \vdash C[w'']}{\Gamma \vdash C[w'']}\ \Diamond E_{bad}$$

This definition can lead to logical inconsistency because the hypothetical judgment $\Gamma \vdash A[w']$ occurs to the left of an arrow in a rule that is ostensibly defining the hypothetical judgment. In **DML** this was no issue: we stipulated that the accessibility relation was definable independently from the hypothetical judgment.

To make the definition of constructive provability logic well-formed, we take the position that the hypothetical judgment $\Gamma \vdash A[w]$ is defined one world at a time. If we then restrict the accessibility relation so that it is *converse well-founded* (irreflexive, no cycles or infinite ascending chains), when $w \prec w'$, then we can hope to define $\Gamma \vdash A[w']$ before $\Gamma \vdash A[w]$ in the same way we defined the accessibility relation $w \prec w'$ before $\Gamma \vdash A[w]$ in **DML**.

If we are trying to define provability one world at a time, the problem with $\Diamond E_{bad}$ is the relationship (or lack thereof) between $\Gamma \vdash A[w']$, which we are reflecting over, and $\Gamma \vdash C[w'']$, which we are defining. To fix this, we must ensure that w' is accessible from w'' in one or more steps, and therefore defined before w''. There are two obvious ways to do this, which give rise to the two variants of constructive provability logic, **CPL** and **CPL***.

1.3.3 *Tethered constructive provability logic.* Because $w \prec w'$, the simplest solution is to force w to be equal to w''; this results in the following "tethered" (in the sense that the world in the premise $\Diamond A[w]$ is tethered to the conclusion $C[w]$) rule for modal possibility:

$$\frac{\Gamma \vdash \Diamond A[w] \quad \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w'] \longrightarrow \Gamma \vdash C[w]}{\Gamma \vdash C[w]}\ \Diamond E_{\mathbf{CPL}}$$

We call this tethered version of constructive provability logic **CPL**, and show the rules for modal necessity to be locally sound and complete in Section 2.

1.3.4 *De-tethered constructive provability logic.* The tethered proof theory of **CPL** can be viewed as unnecessarily restrictive. To fix the inconsistent left rule $\Diamond E_{bad}$, all that is really necessary according to the discussion above is for provability at w' to be defined before provability at w''. We can "de-tether" the logic somewhat by allowing both the case where w is the same as w'' and the case where w is transitively accessible from w'' (this is achieved by adding a premise $w'' \prec^* w$). This is sufficient to ensure that w' will be transitively accessible from w'' ($w'' \prec^{+} w'$), ensuring that provability at w' will be defined before provability at w'' as required. The de-tethered elimination rule for modal possibility in constructive provability logic looks like this:

$$\frac{w'' \prec^{*} w \quad \Gamma \overset{*}{\vdash} \Diamond A[w] \quad \forall w'.\, w \prec w' \longrightarrow \Gamma \overset{*}{\vdash} A[w'] \longrightarrow \Gamma \overset{*}{\vdash} C[w'']}{\Gamma \overset{*}{\vdash} C[w'']} \ \Diamond E_{\mathbf{CPL*}}$$

We call the de-tethered variant of constructive provability logic **CPL***. To distinguish the two similar logics, in the subsequent discussion we will write the hypothetical judgment for **CPL** as $\Gamma \vdash A[w]$ and write the hypothetical judgment for **CPL*** as $\Gamma \overset{*}{\vdash} A[w]$.

1.4 A note on formalization

Both variants of constructive provability logic and their metatheory have been formalized in the Agda proof assistant, an implementation of the constructive type theory of Martin Löf [Norell 2007]. This development is available from `https://github.com/robsimmons/agda-lib/tree/cpl`.

With two exceptions, all of the results in this paper are fully verified by Agda. The most significant exception is that Agda cannot verify that rules such as $\Diamond E_{\mathbf{CPL}}$ and $\Diamond E_{\mathbf{CPL*}}$ above avoid logical inconsistency. This is because Agda's positivity checker, which ensures that data-types are not self-referential, does not understand the critical relationship between the logical rules and the converse well-founded accessibility relation. The result is that the positivity checker must be disabled when we encode the definitions of **CPL** and **CPL***. This issue is discussed further in the technical report along with potential resolutions [Simmons and Toninho 2010]. One key point is that any finite accessibility relation can be instantiated without running afoul of the positivity issue, so we can restrict any concerns to instantiations of constructive provability logic with infinite converse well-founded accessibility relations.

The second issue is that, due to the complexity of the de-tethered cut admissibility proof, Agda runs out of memory and crashes when attempting to verify that this proof terminates. Therefore, we must turn off the termination checker when dealing with this proof. Arguably, this shortcoming is due to the fact that Agda does not allow the user to specify an induction metric – rather, it synthesizes all possible induction metrics and then checks them. However, we can state an induction metric and verify by hand that this induction metric is obeyed in the proof.

2. **CPL**, TETHERED CONSTRUCTIVE PROVABILITY LOGIC

In this section, we will present the defining principles, natural deduction, and sequent calculus for the tethered variant of constructive provability logic, **CPL**. Mirroring the tethered presentation of rules outlined in Section 1.3.3, the substitution principle in **CPL** is tethered: the hypothesis being discharged, $A[w]$, is at the same world as the consequent $C[w]$.

Defining principles of **CPL***:*

—*Hypothesis principle*: If $A[w] \in \Gamma$, then $\Gamma \vdash A[w]$.

$$\dfrac{}{\Gamma, A[w] \vdash A[w]}\ hyp \qquad \dfrac{\Gamma \vdash \bot[w]}{\Gamma \vdash C[w]}\ \bot E$$

$$\dfrac{\Gamma, A[w] \vdash B[w]}{\Gamma \vdash A \supset B[w]}\ {\supset} I \qquad \dfrac{\Gamma \vdash A \supset B[w] \quad \Gamma \vdash A[w]}{\Gamma \vdash B[w]}\ {\supset} E$$

$$\dfrac{w \prec w' \quad \Gamma \vdash A[w']}{\Gamma \vdash \Diamond A[w]}\ \Diamond I \qquad \dfrac{\forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w']}{\Gamma \vdash \Box A[w]}\ \Box I$$

$$\dfrac{\Gamma \vdash \Diamond A[w] \quad \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w'] \longrightarrow \Gamma \vdash C[w]}{\Gamma \vdash C[w]}\ \Diamond E$$

$$\dfrac{\Gamma \vdash \Box A[w] \quad (\forall w'.\, w \prec w' \longrightarrow \Gamma \vdash A[w']) \longrightarrow \Gamma \vdash C[w]}{\Gamma \vdash C[w]}\ \Box E$$

Fig. 1. Intuitionistic **CPL** natural deduction

—*Generalized weakening principle*: If $\Gamma \subseteq_w \Gamma'$ and $\Gamma \vdash A[w]$, then $\Gamma' \vdash A[w]$.

—*Substitution principle*: If $\Gamma \vdash A[w]$ and $\Gamma, A[w] \vdash C[w]$, then $\Gamma \vdash C[w]$.

The natural deduction rules for **CPL** are presented in Fig. 1. Implication, atomic propositions and falsehood are defined as per usual in natural deduction presentations of logic. The introduction rule for modal possibility is visually the same as the rule from **DML**, and the elimination rule was presented in Section 1.3.3, but we have yet to show these rules locally sound and complete. Local soundness is witnessed by the following reduction; as in the local soundness proof for possibility in **DML**, the higher-order proof $\mathcal{D}_3$ is used as a function – we apply it to w', $\mathcal{A}_1$, and $\mathcal{D}_2$ in order to obtain the necessary proof:

$$\dfrac{\dfrac{\overset{\mathcal{A}_1}{w \prec w'} \quad \overset{\mathcal{D}_2}{\Gamma \vdash A[w']}}{\Gamma \vdash \Diamond A[w]}\ \Diamond I \qquad \overset{\mathcal{D}_3}{\forall w'.w \prec w' \longrightarrow \Gamma \vdash A[w'] \longrightarrow \Gamma \vdash C[w]}}{\Gamma \vdash C[w]}\ \Diamond E$$

$$\Longrightarrow_R \quad \begin{array}{c} \mathcal{D}_3\, w'\, \mathcal{A}_1\, \mathcal{D}_2 \\ \Gamma \vdash C[w] \end{array}$$

Local completeness also holds for modal possibility, although the expansion that witnesses the property is somewhat surprising:

$$\begin{array}{c} \mathcal{D} \\ \Gamma \vdash \Diamond A[w] \end{array} \quad \Longrightarrow_E \quad \dfrac{\overset{\mathcal{D}}{\Gamma \vdash \Diamond A[w]} \quad \Diamond I}{\Gamma \vdash \Diamond A[w]}\ \Diamond E$$

We expand a proof of $\Diamond A[w]$ by applying $\Diamond E$ to the given derivation *and* to the actual rule of $\Diamond I$. The higher-order premise for $\Diamond E$ for this proof requires us to prove the following meta-theorem: "If $w \prec w'$ and $\Gamma \vdash A[w']$ then $\Gamma \vdash \Diamond A[w]$." This theorem is immediately true by application of the $\Diamond I$ rule to the assumptions.

All that remains is a discussion of modal necessity. Whereas modal possibility has an existential character (there *exists* some accessible world where A is true), modal necessity has a universal character (at *every* accessible world, A is true). We conclude $\Box A$ at world w if we can show that for all worlds w' that are accessible from w, A is provable at w'; this is reflected in the $\Box I$ rule.

The universal character of modal necessity would suggest that we can *use* a proof of $\Box A[w]$ by exhibiting a world w' accessible from w and then assuming that A was provable there.

$$\frac{\Gamma \vdash \Box A[w] \qquad w \prec w' \qquad \Gamma \vdash A[w'] \longrightarrow \Gamma \vdash C[w]}{\Gamma \vdash C[w]}\,\Box E'$$

Surprisingly, this rule is locally sound but not locally complete in the presence of potentially infinite accessibility relations (consider an infinitely branching accessibility relation – this would require infinite applications of $\Box E'$ in order to obtain enough to information to re-apply $\Box I$), so **CPL** uses a less intuitive third-order formulation of $\Box E$ shown in Fig. 1. The more intuitive rule is nevertheless derivable from the actual $\Box E$ rule, and the third-order formulation of the rule is derivable from $\Box E'$ under the assumption that we can finitely enumerate the worlds accessible from any world (this is established in the file `AltBoxE.agda` in the Agda development).

As per usual in our development, we show our rules to be locally sound, as witnessed by the following reduction:

$$\dfrac{\dfrac{\overset{\mathcal{D}_1}{\forall w'.w \prec w' \longrightarrow \Gamma \vdash A[w']}}{\Gamma \vdash \Box A[w]}\,\Box I \qquad \overset{\mathcal{D}_2}{(\forall w'.w \prec w' \longrightarrow \Gamma \vdash A[w']) \longrightarrow \Gamma \vdash C[w]}}{\Gamma \vdash C[w]}\,\Box E$$

$$\Longrightarrow_R \quad \overset{\mathcal{D}_2\,\mathcal{D}_1}{\Gamma \vdash C[w]}$$

Local completeness for modal necessity is the same as it was for modal possibility; the second premise of the $\Box E$ rule essentially restates the $\Box I$ rule.

Having shown our system to be locally sound and complete, we must now circle back around to show that the judgmental principles hold:

Theorem 1 Metatheory of **CPL** natural deduction.

—*Hypothesis principle: If* $A[w] \in \Gamma$*, then* $\Gamma \vdash A[w]$.

—*Generalized weakening principle: If* $\Gamma \subseteq_w \Gamma'$ *and* $\Gamma \vdash A[w]$*, then* $\Gamma' \vdash A[w]$.

—*Substitution principle: If* $\Gamma \vdash A[w]$ *and* $\Gamma, A[w] \vdash C[w]$*, then* $\Gamma \vdash C[w]$.

Proof. The hypothesis principle follows immediately from the rule *hyp*. The generalized weakening principle is established by structural induction on given derivation, and the substitution principle is established by structural induction on the second given derivation $\Gamma, A[w] \vdash C[w]$. Both proofs appear in `TetheredCPL/NatDeduction.agda` in the Agda development. □

2.1 Sequent calculus

Often we want to be able to show that a judgment is not provable in a logic (for instance, we better not be able to derive the judgment $\cdot \vdash \bot[w]$, which would represent a closed contradiction). While natural deduction is a canonical way of thinking about proofs, it is not very useful as a tool for proving such negative statements about logic. This is largely because natural deduction does not obey the

$$\frac{}{\Gamma, Q[w] \Rightarrow Q[w]}\ \mathit{init} \quad (Q \text{ is an atomic proposition}) \quad \frac{\bot[w] \in \Gamma}{\Gamma \Rightarrow C[w]}\ \bot L$$

$$\frac{\Gamma, A[w] \Rightarrow B[w]}{\Gamma \Rightarrow A \supset B[w]}\ {\supset}R \quad \frac{A \supset B[w] \in \Gamma \quad \Gamma \Rightarrow A[w] \quad \Gamma, B[w] \Rightarrow C[w]}{\Gamma \Rightarrow C[w]}\ {\supset}L$$

$$\frac{w \prec w' \quad \Gamma \Rightarrow A[w']}{\Gamma \Rightarrow \Diamond A[w]}\ \Diamond R \quad \frac{\forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']}{\Gamma \Rightarrow \Box A[w]}\ \Box R$$

$$\frac{\Diamond A[w] \in \Gamma \quad \forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w'] \longrightarrow \Gamma \Rightarrow C[w]}{\Gamma \Rightarrow C[w]}\ \Diamond L$$

$$\frac{\Box A[w] \in \Gamma \quad (\forall w'.\, w \prec w' \longrightarrow \Gamma \Rightarrow A[w']) \longrightarrow \Gamma \Rightarrow C[w]}{\Gamma \Rightarrow C[w]}\ \Box L$$

Fig. 2. Sequent calculus for intuitionistic **CPL**

so-called *sub-formula property* (all judgments in a proof refer only to sub-formulas of the propositions present in the initial judgment). A sequent calculus system, on the other hand, obeys the sub-formula property and therefore allows us to prove negative statements about a logic by refutation: we assume the sequent is provable and, by case analysis on the structure of the derivation, derive a contradiction. The sequent calculus for **CPL** is given in Fig. 2.

Even though sequent calculus systems are structured quite differently than natural deduction systems, we can (and must!) establish the admissibility of the same defining principles.

THEOREM 2 METATHEORY OF THE **CPL** SEQUENT CALCULUS.

—*Hypothesis principle: If* $A[w_i] \in \Gamma$*, then* $\Gamma \Rightarrow A[w_i]$.

—*Generalized weakening principle: If* $\Gamma \subseteq_w \Gamma'$ *and* $\Gamma \Rightarrow A[w]$*, then* $\Gamma' \Rightarrow A[w]$.

—*Substitution principle: If* $\Gamma \Rightarrow A[w]$ *and* $\Gamma, A[w] \Rightarrow C[w]$*, then* $\Gamma \Rightarrow C[w]$.

PROOF. The hypothesis principle is established by structural induction on the proposition A, and the generalized weakening principle is established by structural induction on the given derivation. The substitution principle is proved by lexicographic induction, primarily on the structure of the proposition A and secondarily on the structures of both given derivations: if the proposition A stays the same, then either the first derivation gets smaller and the second stays the same or the second derivation gets smaller and the first stays the same. All proofs appear in `TetheredCPL/Sequent.agda` in the Agda development. □

In sequent calculi, the hypothesis principle is frequently called *identity admissibility* and the substitution principle is frequently called *cut admissibility*. The admissibility of cut and identity establish the global analogues of local soundness and completeness, respectively.

By presenting a sequent calculus system as a convenient way of establishing non-provability of hypothetical judgments in a natural deduction system, we have presupposed that the two presentations are equivalent. Luckily, we were right:

THEOREM 3 EQUIVALENCE. $\Gamma \vdash A[w]$ *if and only if* $\Gamma \Rightarrow A[w]$.

$$\dfrac{}{\Gamma, A[w] \vdash^{*} A[w]}\ \mathit{hyp} \qquad \dfrac{w' \prec^{*} w \quad \Gamma \vdash^{*} \bot[w]}{\Gamma \vdash^{*} C[w']}\ \bot E$$

$$\dfrac{\Gamma, A[w] \vdash^{*} B[w]}{\Gamma \vdash^{*} A \supset B[w]}\ {\supset}I \qquad \dfrac{\Gamma \vdash^{*} A \supset B[w] \quad \Gamma \vdash^{*} A[w]}{\Gamma \vdash^{*} B[w]}\ {\supset}E$$

$$\dfrac{w \prec w' \quad \Gamma \vdash^{*} A[w']}{\Gamma \vdash^{*} \Diamond A[w]}\ \Diamond I \qquad \dfrac{\forall w'.\, w \prec w' \longrightarrow \Gamma \vdash^{*} A[w']}{\Gamma \vdash^{*} \Box A[w]}\ \Box I$$

$$\dfrac{w'' \prec^{*} w \quad \Gamma \vdash^{*} \Diamond A[w] \quad \forall w'.\, w \prec w' \longrightarrow \Gamma \vdash^{*} A[w'] \longrightarrow \Gamma \vdash^{*} C[w'']}{\Gamma \vdash^{*} C[w'']}\ \Diamond E$$

$$\dfrac{w'' \prec^{*} w \quad \Gamma \vdash^{*} \Box A[w] \quad (\forall w'.\, w \prec w' \longrightarrow \Gamma \vdash^{*} A[w']) \longrightarrow \Gamma \vdash^{*} C[w'']}{\Gamma \vdash^{*} C[w'']}\ \Box E$$

Fig. 3. Intuitionistic **CPL*** natural deduction

Proof. Both directions must be proved simultaneously, primarily by induction on the accessibility relation and secondarily by structural induction on the given derivation. The defining principles of the sequent calculus presentation (Theorem 2) are used in the forward direction, and the defining principles of the natural deduction presentation (Theorem 1) are used in the backward direction. The proof appears in `TetheredCPL/Equiv.agda` in the Agda development. □

2.2 Example

We now formalize the example that motivated Section 1.3, showing that the sequent $\Diamond Q[\alpha] \Rightarrow \bot[\alpha]$ is derivable (and by the equivalence of natural deduction and sequent calculus, that $\Diamond Q[\alpha] \vdash \bot[\alpha]$ is derivable). The last rule in our proof will be $\Diamond L$:

$$\dfrac{\forall w'.\, \alpha \prec w' \longrightarrow \Diamond Q[\alpha] \overset{\mathcal{E}}{\Rightarrow} Q[w'] \longrightarrow \Diamond Q[\alpha] \Rightarrow \bot[\alpha]}{\Diamond Q[\alpha] \Rightarrow \bot[\alpha]}\ \Diamond L$$

Therefore, it suffices to show that for all w' accessible from α, $\Diamond Q[\alpha] \Rightarrow Q[w']$ implies $\Diamond Q[\alpha] \Rightarrow \bot[\alpha]$. In this running example, there are two worlds β and γ accessible from α, so we must show that $\Diamond Q[\alpha] \Rightarrow Q[\beta]$ implies $\Diamond Q[\alpha] \Rightarrow \bot[\alpha]$ and that $\Diamond Q[\alpha] \Rightarrow Q[\gamma]$ implies $\Diamond Q[\alpha] \Rightarrow \bot[\alpha]$. The reasoning in both cases is exactly the same; we'll prove only the first here.

The way we prove that $\Diamond Q[\alpha] \Rightarrow Q[\beta]$ implies $\Diamond Q[\alpha] \Rightarrow \bot[\alpha]$ is to prove that there is *no* proof of $\Diamond Q[\alpha] \Rightarrow Q[\beta]$, which means that the implication holds vacuously. To prove this, we assume $\Diamond Q[\alpha] \Rightarrow Q[\beta]$ is derivable. The only possible rule that could potentially allow us to conclude this sequent is $\Diamond L$, since there is no $Q[\beta]$ in the context in order to apply the *init* rule. However, since the worlds α and β do not match, the rule does not apply and the sequent is not provable.

3. **CPL***, DE-TETHERED CONSTRUCTIVE PROVABILITY LOGIC

The natural deduction rules for **CPL*** are presented in Figure 3. The only difference from the corresponding rules of the previous section is that we no longer restrict the conclusion of elimination rules to be at the world w of the judgment we are eliminating, instead allowing it to be at a world w'', provided that $w'' \prec^* w$ (an exception is $\supset E$, since the rule does not mention an arbitrary proposition C).

The proofs of local soundness and completeness are analogous to the ones discussed in the previous section; the substitution principle is de-tethered in the same way that the elimination rules are.

Theorem 4 Metatheory of **CPL*** natural deduction.

—*Hypothesis principle: If* $A[w] \in \Gamma$, *then* $\Gamma \overset{*}{\vdash} A[w]$.

—*Generalized weakening principle: If* $\Gamma \subseteq_w \Gamma'$ *and* $\Gamma \overset{*}{\vdash} A[w]$, *then* $\Gamma' \overset{*}{\vdash} A[w]$.

—*Substitution principle: If* $w' \prec^* w$, $\Gamma \overset{*}{\vdash} A[w]$, *and* $\Gamma, A[w] \overset{*}{\vdash} C[w']$, *then* $\Gamma \overset{*}{\vdash} C[w']$.

Proof. The hypothesis principle again follows immediately from the rule *hyp*. The generalized weakening principle is established by a primary induction on the accessibility relation and a secondary structural induction on the given derivation. The substitution principle is established by a primary induction on the accessibility relation and then a secondary structural induction on the second given derivation $\Gamma, A[w] \overset{*}{\vdash} C[w']$. Both proofs appear in `DetetheredCPL/NatDeduction.agda` in the Agda development. □

3.1 Focused sequent calculus

The sequent calculus formulation of **CPL** is convenient for establishing very simple properties of provability and non-provability, and it is possible to give a very similar sequent calculus for **CPL*** [Simmons and Toninho 2011]. However, because we wish to consider **CPL*** as the basis of a logic programming language, we follow Andreoli [1992] in developing a much more restricted *focused* sequent calculus. Unlike Andreoli, we use an explicitly polarized version of our logic.

Propositions in a polarized presentation of logic are split into two syntactic categories, *positive* propositions A^+ and *negative* propositions A^-. A full discussion of polarity assignment for connectives is outside the scope of this article; as a rule of thumb, the *positive* connectives are those with large eliminations. An elimination is large when the proposition whose truth is established by an elimination rule is some proposition C with no immediate connection to the proposition being eliminated; this indicates that $\bot$, $\Diamond A$, and $\Box A$ are positive connectives and $A \supset B$ is not.

$$
\begin{array}{rcl}
A^+, B^+ & ::= & Q^+ \mid {\downarrow}A^- \mid \bot \mid \Diamond A^+ \mid \Box A^+ \\
A^-, B^- & ::= & Q^- \mid {\uparrow}A^+ \mid A^+ \supset B^-
\end{array}
$$

Each atomic proposition can be positive or negative, but never both, as if each atomic proposition in the un-polarized logic was always already intrinsically positive or negative and our previous natural deduction and sequent calculi were unable to notice.

Both of the modal operators in constructive provability logic are naturally positive on the *outside*. However, our choice of the polarity for the proposition *inside* the modality appears to be arbitrary: $\Diamond A^+$ and $\Diamond A^-$ would both be reasonable ways to polarize the possibility modality. Polarization of propositions is a property that affects *proofs*, not *provability*, so the modalities $\Diamond A$ and $\Box A$, which, in constructive provability logic, only care about the provability of the sub-formula A, are naturally indifferent to the treatment of A as a positive or negative proposition.

$$\boxed{\Gamma \overset{*}{\Rrightarrow} \llbracket C^-[w] \rrbracket}$$

$$\frac{}{\Gamma, Q^+[w] \overset{*}{\Rrightarrow} \llbracket Q^+[w] \rrbracket}\ QR^+ \qquad \frac{\Gamma; \cdot \overset{*}{\Rrightarrow} A^-[w]}{\Gamma \overset{*}{\Rrightarrow} \llbracket {\downarrow} A^-[w] \rrbracket}\ {\downarrow}R$$

$$\frac{w \prec w' \quad \Gamma; \cdot \overset{*}{\Rrightarrow} {\uparrow}A^+[w']}{\Gamma \overset{*}{\Rrightarrow} \llbracket \Diamond A^+[w] \rrbracket}\ \Diamond R \qquad \frac{\forall w'. w \prec w' \longrightarrow \Gamma; \cdot \overset{*}{\Rrightarrow} {\uparrow}A^+[w']}{\Gamma \overset{*}{\Rrightarrow} \llbracket \Box A^+[w] \rrbracket}\ \Box R$$

$$\boxed{\Gamma; \cdot \overset{*}{\Rrightarrow} C^-[w]}$$

$$\frac{}{Q^+\ \mathit{stable}^+} \qquad \frac{}{{\downarrow}A^-\ \mathit{stable}^+} \qquad \frac{}{Q^-\ \mathit{stable}^-} \qquad \frac{}{{\uparrow}A^+\ \mathit{stable}^-}$$

$$\frac{\Gamma; A^+[w] \overset{*}{\Rrightarrow} B^-[w]}{\Gamma; \cdot \overset{*}{\Rrightarrow} A^+ \supset B^-[w]}\ {\supset}R \qquad \frac{A^+\ \mathit{stable}^+ \quad \Gamma, A^+[w']; \cdot \overset{*}{\Rrightarrow} C^-[w]}{\Gamma; A^-[w'] \overset{*}{\Rrightarrow} C^-[w]}\ L$$

$$\frac{C^-\ \mathit{stable}^- \quad w \prec^* w' \quad \Gamma, {\downarrow}A^-[w'] \overset{*}{\Rrightarrow} A^-[w'] \gg C^-[w]}{\Gamma, {\downarrow}A^-[w']; \cdot \overset{*}{\Rrightarrow} C^-[w]}\ {\downarrow}L$$

$$\frac{}{\Gamma; \bot[w'] \overset{*}{\Rrightarrow} C^-[w]}\ \bot L \qquad \frac{\forall w. w' \prec w \longrightarrow \Gamma; \cdot \overset{*}{\Rrightarrow} {\uparrow}A^+[w] \longrightarrow \Gamma; \cdot \overset{*}{\Rrightarrow} C^-[w'']}{\Gamma; \Diamond A^+[w'] \overset{*}{\Rrightarrow} C^-[w'']}\ \Diamond L$$

$$\frac{(\forall w. w' \prec w \longrightarrow \Gamma; \cdot \overset{*}{\Rrightarrow} {\uparrow}A^+[w]) \longrightarrow \Gamma; \cdot \overset{*}{\Rrightarrow} C^-[w'']}{\Gamma; \Box A^+[w'] \overset{*}{\Rrightarrow} C^-[w'']}\ \Box L \qquad \frac{\Gamma \overset{*}{\Rrightarrow} \llbracket A^+[w] \rrbracket}{\Gamma; \cdot \overset{*}{\Rrightarrow} {\uparrow}A^+[w]}\ {\uparrow}R$$

$$\boxed{\Gamma \overset{*}{\Rrightarrow} A^-[w'] \gg C^-[w]}$$

$$\frac{}{\Gamma \overset{*}{\Rrightarrow} Q^-[w] \gg Q^-[w]}\ QL^- \qquad \frac{\Gamma; A^+[w'] \overset{*}{\Rrightarrow} C^-[w]}{\Gamma \overset{*}{\Rrightarrow} {\uparrow}A^+[w'] \gg C^-[w]}\ {\uparrow}L$$

$$\frac{\Gamma \overset{*}{\Rrightarrow} \llbracket A^+[w'] \rrbracket \quad \Gamma \overset{*}{\Rrightarrow} B^-[w'] \gg C^-[w]}{\Gamma \overset{*}{\Rrightarrow} A^+ \supset B^-[w'] \gg C^-[w]}\ {\supset}L$$

Fig. 4. Focused sequent calculus for intuitionistic **CPL***

To develop the focused calculus, we require three types of sequent: a *right focus* sequent $\Gamma \overset{*}{\Rrightarrow} \llbracket A^+[w] \rrbracket$, describing a state where non-invertible right rules are applied to positive propositions; a *left focus* sequent $\Gamma \overset{*}{\Rrightarrow} A^-[w'] \gg C^-[w]$, where non-invertible left rules are applied to negative propositions (we typically say that the proposition A^- is under focus); and an *inversion* sequent $\Gamma; \Omega \overset{*}{\Rrightarrow} A^-[w]$, describing everything else (the additional context Ω, which is either $\cdot$ or a single judgment $A^+[w]$, is called the *inversion context*). We define the system in such a way that whenever the inversion context is non-empty, there is only one applicable rule – the one that decomposes the connective in the inversion context. We require two additional judgments, $A^+\ \mathit{stable}^+$ and $A^-\ \mathit{stable}^-$, which restrict the inversion phase. The rules defining the focused **CPL*** sequent calculus are given in Fig. 4.

Validating the judgmental principles is quite complex in focused **CPL***; the proof adapts techniques used in the analogous proofs for **CPL** as well as the *structural focalization* techniques described by Simmons [2011]. The generalized weakening principle is established in `FocusedCPL/Weakening.agda`. The substitution principle is established as a corollary of the cut admissibility, which is established in `FocusedCPL/Cut.agda`. Notably, in order to prove the substitution theorem, we

$$
\begin{array}{rcl}
 & & (\cdot)^{\circledcirc} = \cdot \\
(Q^{+})^{\oplus} = Q^{+} & (Q^{+})^{\ominus} = {\uparrow}Q^{+} & (\Gamma, Q^{+}[w])^{\circledcirc} = \Gamma^{\circledcirc}, Q^{+}[w] \\
(\bot)^{\oplus} = \bot & (\bot)^{\ominus} = {\uparrow}\bot & (\Gamma, \bot[w])^{\circledcirc} = \Gamma^{\circledcirc}, {\downarrow}{\uparrow}\bot[w] \\
(\Diamond A)^{\oplus} = \Diamond A^{\oplus} & (\Diamond A)^{\ominus} = {\uparrow}(\Diamond A^{\oplus}) & (\Gamma, \Diamond A[w])^{\circledcirc} = \Gamma^{\circledcirc}, {\downarrow}{\uparrow}(\Diamond A^{\oplus})[w] \\
(\Box A)^{\oplus} = \Box A^{\oplus} & (\Box A)^{\ominus} = {\uparrow}(\Box A^{\oplus}) & (\Gamma, \Box A[w])^{\circledcirc} = \Gamma^{\circledcirc}, {\downarrow}{\uparrow}(\Box A^{\oplus})[w] \\
(Q^{-})^{\oplus} = {\downarrow}Q^{-} & (Q^{-})^{\ominus} = Q^{-} & (\Gamma, Q^{-}[w])^{\circledcirc} = \Gamma^{\circledcirc}, {\downarrow}Q^{-}[w] \\
(A \supset B)^{\oplus} = {\downarrow}(A^{\oplus} \supset B^{\ominus}) & (A \supset B)^{\ominus} = A^{\oplus} \supset B^{\ominus} & (\Gamma, A \supset B[w])^{\circledcirc} = \Gamma^{\circledcirc}, {\downarrow}(A^{\oplus} \supset B^{\ominus})[w]
\end{array}
$$

Fig. 5. Polarization of propositions and contexts

must simultaneously prove a a *backwards* substitution theorem establishing that $\Gamma; \cdot \overset{*}{\Rrightarrow} A[w]$ and $\Gamma; \cdot \overset{*}{\Rrightarrow} C[w']$ together imply $\Gamma; \cdot \overset{*}{\Rrightarrow} C[w']$; this fact does not follow from generalized weakening when $w' \prec^{+} w$. Finally, the hypothesis principle is established as a corollary of identity expansion in `FocusedCPL/Identity.agda`.

We only establish a weak form of equivalence between the focused sequent calculus and the natural deduction system; we define a polarization strategy (Figure 5) that maps unpolarized propositions and contexts to polarized ones. It is more robust to define equivalence on the basis of *erasing* polarized propositions and contexts to unpolarized ones [Simmons 2011], but this formulation is sufficient for our purposes.

THEOREM 5 EQUIVALENCE. $\Gamma \overset{*}{\vDash} A[w]$ *if and only if* $\Gamma^{\circledcirc}; \cdot \overset{*}{\Rrightarrow} A^{\ominus}[w]$

PROOF. Both directions must be proved simultaneously, primarily by induction on the accessibility relation and secondarily by structural induction on the given derivation. The forward direction uses the metatheory of the focused sequent calculus and is structured similarly to the proof in [Simmons 2011], and the reverse direction uses the defining principles of the natural deduction system (Theorem 4). The proof appears in `DetetheredCPL/Equiv.agda` in the Agda development. □

4. LOGIC PROGRAMMING IN CONSTRUCTIVE PROVABILITY LOGIC

Proving the natural deduction system for **CPL*** equivalent to a focused presentation of the logic is a lot of work, but the payoff is that the focused sequent calculus can form the basis of a logic programming language [Miller et al. 1991; Andreoli 1992]. We will use an *extremely* simplified example here: translating a propositional Horn clause logic program with stratified negation where there are only two strata. In this section, atomic propositions in the first strata will be written with the metavariable Q, and atomic propositions in the second strata will be written with the metavariable P.

Atomic propositions Q can appear at the head of Horn clauses of the form Q `:-` $Q_1, \ldots, Q_n$ in the logic program; atomic propositions P can appear at the head of Horn clauses of the form P `:-` $A_1, \ldots, A_n$ in the logic program, where each A_i is either an atomic proposition P_i, an atomic proposition Q_i, or a negated atomic proposition $\neg Q_i$. We will use the worlds β and γ (where $\beta \prec \gamma$) from our running example. Each first-strata Horn clause Q `:-` $Q_1, \ldots, Q_n$ is translated into a judgment ${\downarrow}(Q_1 \supset \ldots \supset Q_n \supset {\uparrow}Q)[\gamma]$, and each second-strata Horn clause

P :- $A_1, \ldots, A_n$ is translated into a judgment $\downarrow(A_1^\bullet \supset \ldots \supset A_n^\bullet \supset \uparrow P)[\beta]$, where $(P_i)^\bullet = P_i$, $(Q_i)^\bullet = \Box Q_i$, and $(\neg Q_i)^\bullet = \downarrow((\Box Q_i) \supset \uparrow\bot)$. (Note that this implies a positive polarity for all atomic propositions.) We name the context obtained by translating our Horn clause logic program Γ.

Searching for a proof of a proposition P using bottom-up logic programming can be characterized as a two phase proof search procedure for proofs of the term $\Gamma, \Gamma'; \cdot \overset{*}{\Rrightarrow} \uparrow P[\beta]$, where we always maintain the invariant that $\Gamma, \Gamma'; \cdot \overset{*}{\Rrightarrow} \uparrow P[\beta]$ is provable if and only if $\Gamma; \cdot \overset{*}{\Rrightarrow} \uparrow P[\beta]$ is provable.

In the first phase, we only focus on hypotheses in Γ with the form $\downarrow(Q_1 \supset \ldots \supset Q_n \supset \uparrow Q)[\gamma]$. Because focusing on such a proposition will succeed exactly when $Q_i[\gamma] \in \Gamma'$ for each of the Q_i, it is always possible to determine the entire set of Q_k that are *immediate consequences* of the rules in Γ and atomic propositions in Γ'. Given a sequent $\Gamma, \Gamma'; \cdot \overset{*}{\Rrightarrow} \uparrow P[\beta]$ that is true if and only if $\Gamma; \cdot \overset{*}{\Rrightarrow} \uparrow P[\beta]$, we determine the immediate (first-strata) consequences Γ_{imm} of (Γ, Γ'). By repeated focusing steps, we can show $\Gamma, (\Gamma' \cup \Gamma_{imm}); \cdot \overset{*}{\Rrightarrow} \uparrow P[\beta]$ implies $\Gamma, \Gamma'; \cdot \overset{*}{\Rrightarrow} \uparrow P[\beta]$, and we can show the converse by the reverse substitution principle discussed in the previous section. This in turns means that we have a new sequent $\Gamma, (\Gamma' \cup \Gamma_{imm}); \cdot \overset{*}{\Rrightarrow} \uparrow P[\beta]$ which is true if and only if $\Gamma; \cdot \overset{*}{\Rrightarrow} \uparrow P[\beta]$. If $\Gamma' \not\supseteq \Gamma_{imm}$, we repeat the first phase. Otherwise $\Gamma' \supseteq \Gamma_{imm}$, so all the immediate consequences Q of (Γ, Γ') are already present in Γ'. In this case, we say we have reached *saturation at* γ and continue to the second phase.

The second phase relies on the fact that, if all of the immediate consequences Q of (Γ, Γ') are already present in Γ', then $\Gamma, \Gamma'; \cdot \overset{*}{\Rrightarrow} \uparrow Q[\gamma]$ is provable if and only if $Q[\gamma] \in (\Gamma, \Gamma')$. This means that we have an effective decision procedure for the provability of first-strata propositions Q. Thus, the second phase proceeds the same as the first, focusing instead on hypotheses in Γ with the form $\downarrow(A_1^\bullet \supset \ldots \supset A_n^\bullet \supset \uparrow P)[\beta]$. Focusing on such a rule will succeed exactly when:

—for each $A_i^\bullet = P_i$, $P_i[\beta] \in \Gamma'$,

—for each $A_i^\bullet = \Box Q_i$, $Q_i[\gamma] \in \Gamma'$, and

—for each $A_i^\bullet = \downarrow((\Box Q_i) \supset \uparrow\bot)$, $Q_i[\gamma] \notin \Gamma'$.

Therefore, given that (Γ, Γ') is saturated at γ, we can also determine the entire set of second-strata propositions that are immediate consequences of (Γ, Γ'). We proceed as before, and once we have reached saturation at β as well, we can declare the original sequent $\Gamma; \cdot \overset{*}{\Rrightarrow} \uparrow P[\beta]$ provable if and only if $P[\beta] \in \Gamma'$ for the final saturated Γ'.

5. AXIOMATIC CHARACTERIZATION

In this section, we present a sound Hilbert-style proof theory for **CPL** and **CPL***. The desired interpretation of $\Vdash A$ is that it implies that, for all converse well-founded accessibility relations and contexts Γ, it is the case that $\Gamma \vdash A[w]$ (in **CPL**). Similarly, the desired interpretation of $\overset{*}{\Vdash} A$ is that, for all converse well-founded accessibility relations and contexts Γ, it is the case that $\Gamma \overset{*}{\vDash} A[w]$ (in **CPL***). We will write $\overset{(*)}{\Vdash} A$ to indicate results that hold in both **CPL** and **CPL***.

This section only considers *soundness* results for Hilbert-style reasoning; we do not claim the converse, which would be a *completeness* result. However, when we claim that a particular formula is not an axiom of **CPL** or **CPL***, we always can demonstrate a particular accessibility relation, world, and instance A of the said formula such that there is no proof of $\Gamma \vdash A[w]$ or $\Gamma \Vdash^{*} A[w]$. For instance, $Q[\alpha] \vdash (\neg\Diamond Q \supset \Box\neg Q)[\alpha]$ is unprovable,[2] so the classically true De Morgan axiom $\neg\Diamond A \supset \Box\neg A$ does not hold in **CPL**. Some axioms, like $\Box A \supset \Box\Box A$, only hold in general when the accessibility relation is transitive; these are indicated.

Both proofs and counterexamples for **CPL** and **CPL*** can be found in `TetheredCPL/Axioms.agda` and in `DetetheredCPL/Axioms.agda` (respectively) in the Agda development.

5.1 Intuitionistic modal logic

All of the axioms of intuitionistic propositional logic are true in both variants of constructive provability logic, as are the fundamental rules and axioms of intuitionistic modal logic. It is less clear what other axioms characterize intuitionistic modal logic; some of the axioms of Simpson's **IK** hold in neither Pfenning-Davies **S4** nor in constructive provability logic.

Theorem 6 Intuitionistic modal logic.

(MP) $\Vdash A \supset B$ *and* $\Vdash A$ *imply* $\Vdash B$*, and* $\Vdash^{*} A \supset B$ *and* $\Vdash^{*} A$ *imply* $\Vdash^{*} B$
(I) $\Vdash^{\wp} A \supset A$
(K) $\Vdash^{\wp} A \supset B \supset A$
(S) $\Vdash^{\wp} (A \supset B \supset C) \supset (A \supset B) \supset A \supset C$
$(\bot E)$ $\Vdash^{\wp} \bot \supset A$
(NEC) $\Vdash A$ *implies* $\Vdash \Box A$*, and* $\Vdash^{*} A$ *implies* $\Vdash^{*} \Box A$
$(K\Box)$ $\Vdash^{\wp} \Box(A \supset B) \supset \Box A \supset \Box B$
$(K\Diamond)$ $\Vdash^{\wp} \Box(A \supset B) \supset \Diamond A \supset \Diamond B$
$(4\Box)$ $\Vdash^{\wp} \Box A \supset \Box\Box A$ *(if the accessibility relation is transitive)*
$(\Diamond\bot)$ $\Vdash^{*} \neg\Diamond\bot$
$(4\Diamond)$ $\Vdash^{*} \Diamond\Diamond A \supset \Diamond A$ *(if the accessibility relation is transitive)*

$\neg\Diamond\bot$ *is not an axiom of* **CPL***, and* $(\Diamond A \supset \Box B) \supset \Box(A \supset B)$ *is not an axiom of either variant.*

If the accessibility relation is transitive, **CPL*** admits the axioms of Pfenning-Davies **S4**, plus $(\Diamond\bot)$, which holds in **IK** but not in Pfenning-Davies **S4**. We have not been able establish the status of axiom $4\Diamond$ in **CPL**.

Simpson's thesis presents axioms characterizing other properties of accessibility relations besides transitivity, but all these properties (e.g. symmetry) are inconsistent with converse well-foundedness, so we ignore them here.

5.2 Provability logic

Exploring the connection between constructive provability logic and provability logic was one of the motivations of this work. The most common characterization of provability logic is the GL axiom. Since GL can be used to prove the $4\Box$ axiom [Verbrugge 2010], it is not surprising that this axiom requires a transitive accessibility relation. The other standard characterization of provability logic is the Löb

[2] $\neg A$ is the usual intuitionistic negation $A \supset \bot$

rule. The Löb rule is almost always presented together with axiom $\mathit{4}\Box$ ensuring transitivity of the accessibility relation, but it is interesting to observe that the Löb rule, unlike the *GL* axiom, holds even without a transitive accessibility relation.

Theorem 7 Provability logic.

(GL) $\Vdash^{\circ} \Box(\Box A \supset A) \supset \Box A$ *(if the accessibility relation is transitive)*
($L\ddot{o}b$) $\Vdash \Box A \supset A$ *implies* $\Vdash A$*, and* $\Vdash^{*} \Box A \supset A$ *implies* $\Vdash^{*} A$

Unlike the proofs of Theorem 6, both parts of Theorem 7 are proved by induction over the accessibility relation.

5.3 De Morgan laws

The interaction between negation and the modal operators is frequently an interesting ground for exploration. In classical modal logic, $\Diamond A$ is just defined as $\neg\Box\neg A$, and so all four of the De Morgan laws – $(\Diamond\neg A \supset \neg\Box A)$, $(\Box\neg A \supset \neg\Diamond A)$, $(\neg\Diamond A \supset \Box\neg A)$, and $(\neg\Box A \supset \Diamond\neg A)$ – hold trivially. The first three hold in Simpson's **IK**, and none hold in Pfenning-Davies **S4**. In **CPL*** two of the four hold, and in **CPL** the same two hold only if we make certain assumptions about consistency at accessible worlds.

Theorem 8 De Morgan laws.

—*In* **CPL****,* $\Vdash^{*} \Diamond\neg A \supset \neg\Box A$ *and* $\Vdash^{*} \Box\neg A \supset \neg\Diamond A$*.*

—*In* **CPL***, neither* $\Diamond\neg A \supset \neg\Box A$ *nor* $\Box\neg A \supset \neg\Diamond A$ *are axioms.*

—*In* **CPL***, both* $\Gamma \Rightarrow \Diamond\neg A \supset \neg\Box A[w]$ *and* $\Gamma \Rightarrow \Box\neg A \supset \neg\Diamond A[w]$ *are true if there is no* $w \prec w'$ *such that* $\Gamma \Rightarrow \bot[w']$*.*

—$\neg\Diamond A \supset \Box\neg A$ *is not an axiom of* **CPL** *or* **CPL****.*

—$\neg\Box A \supset \Diamond\neg A$ *is not an axiom of* **CPL** *or* **CPL****.*

6. CONCLUSION

In this article, we have given natural deduction and sequent calculus presentations for two variants of constructive provability logic, a modal logic with reflection over both accessibility and provability. The standard judgmental principles of all four deductive systems were presented and formalized in the Agda proof assistant (with some caveats described in Section 1.4). Furthermore, through a focused sequent calculus presentation, we produced a sketch of how constructive provability logic can be used as a intuitionistic and proof-theoretic justification for stratified negation in logic programming. Finally, as customary in most works on provability logic, we gave a axiomatic characterization of constructive provability logic and showed that most of the standard axioms of provability logic are sound with respect to our proof theoretic presentation.

6.1 Related work

There has been a substantial amount of research on provability logic throughout the years. The early research on the topic focused on axiomatic presentations of provability logic and its implications for the foundations of mathematics. More recently, there has been interest in the proof theoretic aspects of provability logic, mostly following the cut elimination result of Valentini [1983]. However, most research in provability logic focuses on classical logic (a detailed survey is given in [Artemov and Beklemishev 2004]). Intuitionistic formulations of provability logic have historically been much less explored, with some notable exceptions. For a more detailed historical account of intuitionistic provability logic, as well as a development of a provability logic for intuitionistic arithmetic, see [Iemhoff 2001].

Our line of work departs substantially from previous presentations, even from intuitionistic variants of provability logic. Natural deduction systems for provability logic are also not very common in the literature, given the historical bias towards axiomatic systems. Furthermore, most existing sequent calculi for provability logic are classical, and do not make use of explicit worlds nor reflection, which arise as a natural way of representing provability logic through the judgmental methodology, and thus are substantially different from our own. A focused sequent calculus for provability logic is also, to the best of our knowledge, unheard of.

6.2 Future work

This work introduces propositional constructive logic programming as a modal logic. The only major shortcoming to our treatment of **CPL** and **CPL*** as modal logics is that we do not know how to formulate or prove the completeness of our system with respect to a Hilbert-style presentation. It is not at all clear how this deficiency can be overcome. It may require the introduction of a notion of validity similar to the validity considered by Pfenning and Davies [2001], and it also may require more fundamental changes to the logic, such as making the computational content of the higher order rule formulations more explicit.

In contrast to our relatively thorough investigation of **CPL** and **CPL*** as modal logics, we have only barely scratched the surface of understanding the possible applications of constructive provability logic as the basis for proof search and logic programming. We ultimately wish to use constructive provability logic to justify the L10 logic programming language, a rich forward-chaining language that uses worlds to enable both distributed logic programming and locally stratified negation [Simmons et al. 2011]. To do so, we require a satisfactory treatment of first-order quantification in constructive provability logic, as the account in this paper was entirely propositional. In addition, it is likely that a hybrid modal operator $A@w$ will prove to be more useful than the traditional modal operators $\Diamond A$ and $\Box A$, but this is a minor change from a proof-theoretic perspective.

Horn-clause logic programming is only the simplest logic programming application of constructive provability logic; the focused presentation of **CPL*** immediately opens the door to the principled addition of stratified negation to more interesting logic programming languages, such as higher-order logic programming languages like λProlog and Twelf. We also believe that constructive provability logic with nominal quantification could be presented as a generalization of the Bedwyr language, which synthesizes model checking and logic programming [Baelde et al. 2007].

Finally, provability logic is quite important in other areas of computer science, particularly as the basis for the approximation or delay modality $\triangleright$ used to model programming languages [Nakano 2000; Richards 2010]. We hope to better understand whether and how constructive provability logic can relate to this line of work.

Acknowledgements

Michael Ashley-Rollman, William Lovas, Frank Pfenning, André Platzer, and the reviewers and participants of the 2011 IMLA workshop provided valuable feedback and corrections to earlier versions and drafts of this work.

This work was supported by an X10 Innovation Award from IBM, a National Science Foundation Graduate Research Fellowship for the first author, and by Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) through the Carnegie Mellon Portugal Program under Grants NGN-44 and SFRH / BD / 33763 / 2009.

REFERENCES

Andreoli, J.-M. 1992. Logic programming with focusing proofs in linear logic. *Journal of Logic and Computation 2,* 3, 297–347.

Artemov, S. N. and Beklemishev, L. D. 2004. Provability logic. In *Handbook of Philosophical Logic*, Second ed., D. Gabbay and F. Guenthner, Eds. Vol. 13. 229–403.

Baelde, D., Gacek, A., Miller, D., Nadathur, G., and Tiu, A. 2007. The bedwyr system for model checking over syntactic expressions. In *Automated Deduction (CADE-21)*, F. Pfenning, Ed. Springer LNAI 4603, 391–397.

Gabbay, D. M. 1991. Modal provability foundations for negation by failure. In *Extensions of Logic Programming*, P. Schroeder-Heister, Ed. Springer LNCS 475, 179–222.

Iemhoff, R. 2001. Provability logic and admissible rules. Ph.D. thesis, University of Amsterdam.

Martin-Löf, P. 1996. On the meanings of the logical constants and the justifications of the logical laws. *Nordic Journal of Philosophical Logic 1,* 1, 11–60.

Miller, D., Nadathur, G., Pfenning, F., and Scedrov, A. 1991. Uniform proofs as a foundation for logic programming. *Annals of Pure and Applied Logic 51,* 1–2, 125–157.

Nakano, H. 2000. A modality for recursion. In *Proceedings of the 15th Annual Symposium on Logic in Computer Science (LICS'00)*. Santa Barbara, California, 255–266.

Norell, U. 2007. Towards a practical programming language based on dependent type theory. Ph.D. thesis, Chalmers University of Technology.

Pfenning, F. and Davies, R. 2001. A judgmental reconstruction of modal logic. *Mathematical Structures in Computer Science 11,* 4, 511–540. Notes to an invited talk at the *Workshop on Intuitionistic Modal Logics and Applications (IMLA'99)*, Trento, Italy, July 1999.

Przymusinski, T. C. 1988. On the declarative semantics of deductive databases and logic programs. In *Foundations of deductive databases and logic programming*, J. Minker, Ed. M. Kaufmann Publishers.

Richards, C. D. 2010. The approximation modality in models of higher-order types. Ph.D. thesis, Princeton University.

Schroeder-Heister, P. 1993. Rules of definitional reflection. In *Proceedings of 8th Annual Symposium on Logic in Computer Science (LICS'93)*. Montreal, Quebec, 222–232.

Simmons, R. J. 2011. Structural focalization. *CoRR abs/1109.6273.* Submitted.

Simmons, R. J. and Toninho, B. 2010. Principles of constructive provability logic. Tech. Rep. CMU-CS-10-151, Department of Computer Science, Carnegie Mellon University. Dec.

Simmons, R. J. and Toninho, B. 2011. Constructive provability logic. In *Intuitionstic Modal Logic and Applications.*

Simmons, R. J., Toninho, B., and Pfenning, F. 2011. Distributed deductive databases, declaratively: The L10 logic programming language. In *Proceedings of the X10 Workshop.* ACM.

Simpson, A. K. 1994. The proof theory and semantics of intuitionistic modal logic. Ph.D. thesis, University of Edinburgh.

Valentini, S. 1983. The modal logic of provability: Cut-elimination. *Journal of Philosophical Logic 12,* 4, 471–476.

VERBRUGGE, R. L. 2010. Provability logic. In *The Stanford Encyclopedia of Philosophy*, Winter 2010 ed., E. N. Zalta, Ed.

WHALEY, J., AVOTS, D., CARBIN, M., AND LAM, M. S. 2005. Using datalog with binary decision diagrams for program analysis. In *Programming Languages and Systems (APLAS'05)*, K. Yi, Ed. Springer LNCS 3780, 97–118.

ZEILBERGER, N. 2008. Focusing and higher-order abstract syntax. In *Principles of Programming Languages*. ACM, 359–369.